In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

In the Claims:

Claims 1-10 (Previously cancelled).

11. (Currently amended) An electronic circuit for the securing of a cryptography coprocessor comprising:

a memory module for storing a message to be processed by an encryption or decryption operation and a digital key;

a battery of input/output registers connected to the memory module by a two-way link for receiving digital key data from said memory module comprising the digital key and a plurality of scrambling bits intermixed with the digital key;

said battery of input/output registers comprising a scrambling register for storing the scrambling bits separate from the digital key data;

an input register for receiving the ~~data elements of~~ a message to be processed ~~by an encryption or decryption operation~~;

a key register for receiving the ~~data elements of~~ ~~an encryption or decryption~~ digital key data for use in the encryption or decryption operation;

a multiplexer to carry out a transfer of data between the battery of input/output registers and the input register and the key register;

a processing module ~~to perform~~ connected to said scrambling register, said input register, and said key register for determining the digital key based upon the digital key data in said key register and the scrambling bits in said scrambling register, and for performing the encryption or decryption

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

operation ~~and for receiving~~ on the message ~~to be processed from~~ stored in the input register ~~and for receiving the digital key from the key register to process the message~~ based thereon;

a control module for controlling the memory module, the battery of input/output registers, the multiplexer and the processing module; and

an output register to transmit the result of the encryption or decryption operation to the battery of input/output registers through the multiplexer~~;~~.

~~the battery of input/output registers comprising a scrambling register to receive scrambling bits foreign to the message to be processed or to the digital key.~~

B1

12. (Previously added) An electronic circuit according to Claim 11 wherein the scrambling bits are foreign to the message to be processed and to the digital key.

13. (Currently amended) An electronic circuit according to Claim 11, further comprising an accessory input register connected ~~to the~~ between said processing module and ~~to the multiplexer~~ said scrambling register to receive the scrambling bits ~~from the processing module or from the memory module~~.

14. (Previously added) An electronic circuit according to Claim 13, wherein the accessory input register is the same size as the scrambling register.

15. (Previously added) An electronic circuit according

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

to Claim 11, wherein the scrambling bits are generated randomly.

16. (Previously added) An electronic circuit according to Claim 11, wherein the scrambling bits are sent in groups of eight bits.

17. (Currently amended) An electronic circuit for a cryptography coprocessor comprising:

a plurality of input/output registers having a scrambling register for receiving digital key data comprising a digital key and a plurality of scrambling bits intermixed with the digital key;

B1

an input register for receiving message data to be processed by ~~an~~ the encryption or decryption operation;

a key register for receiving ~~encryption or decryption~~ the digital key data for use in the encryption or decryption operation;

a multiplexer for transferring data between the plurality of input/output registers and the input register and the key register;

a processor connected to said scrambling register, said input register, and said key register for performing the encryption or decryption operation ~~and for receiving~~ on the message data ~~from~~ in the input register ~~and for receiving the key data from the key register~~ based upon the digital key data and the scrambling bits;

a controller for controlling the plurality of input/output registers, the multiplexer and the processor; and

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

an output register to transmit the result of the encryption or decryption operation to the plurality of input/output registers through the multiplexer.

18. (Currently amended) An electronic circuit according to Claim 17 wherein the scrambling bits are foreign to the message data and the digital key ~~data~~.

19. (Currently amended) An electronic circuit according to Claim 17, further comprising an accessory input register connected ~~to the processing module~~ between said processor and ~~to the multiplexer~~ said scrambling register to receive the scrambling bits ~~from the processing module~~.

20. (Previously added) An electronic circuit according to Claim 19, wherein the accessory input register is the same size as the scrambling register.

21. (Currently amended) An electronic circuit according to Claim 17, further comprising: a memory connected to the plurality of input/output registers~~; and~~ for storing the message to be processed and the digital key.

~~an accessory input register connected to the processing module and to the multiplexer for receiving the scrambling bits from the memory.~~

22. (Currently amended) An electronic circuit according to Claim ~~21~~ 19, wherein the accessory input register is the same

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

size as the scrambling register.

23. (Previously added) An electronic circuit according to Claim 17, wherein the scrambling bits are generated randomly.

24. (Previously added) An electronic circuit according to Claim 17, wherein the scrambling bits are sent in groups of eight bits.

25. (Currently amended) A method for securing a cryptography coprocessor comprising ~~the steps of~~:

transmitting data by a two-way link from a memory module to a battery of input/output registers, the battery of input/output registers comprising a scrambling register;

transmitting data corresponding to a message to be processed by an encryption or decryption operation, through a multiplexer, from the battery of input/output registers to an input register; and

transmitting digital key data ~~corresponding to an encryption or decryption digital key~~ for the encryption or decryption operation comprising a digital key and a plurality of scrambling bits intermixed with the digital key, through the multiplexer, from the battery of input/output registers to a key register~~;~~, and ~~transmitting~~ storing the scrambling bits, which are foreign to the message to be processed~~, with~~ and the digital key, ~~to a~~ in the scrambling register of the battery of input/output registers ~~from the memory module or the processing module~~; ~~and~~

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

using a processing module to determine the digital key based upon the digital key data stored in the key register and the scrambling bits stored in the scrambling register; and

~~processing~~ performing the encryption or description operation on the message to be processed stored in the input register with ~~a~~ the processing module based upon the determined digital key ~~receiving the data from the input register, receiving the data from the key register~~, and outputting ~~data corresponding to the processed message~~ the result of the encryption or decryption operation to an output register.

B1

Claim 26 (canceled).

27. (Currently amended) A method according to Claim 25, wherein the scrambling bits are ~~transmitted~~ randomly intermixed with the digital key.

28. (Currently amended) A method according to Claim 25, wherein the scrambling bits are transmitted to the scrambling register whenever ~~a~~ digital key data is input into the battery of input/output registers.

29. (Previously added) A method according to Claim 25, wherein the scrambling bits comprise groups of eight bits.

30. (Currently amended) A method for operating a cryptography coprocessor comprising ~~the steps of~~:

transmitting data to a plurality of input/output

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

registers, the plurality of input/output registers comprising a scrambling register;

transmitting message data to be processed by an encryption or decryption operation, through a multiplexer, from the plurality of input/output registers to an input register; and

transmitting digital key data for the encryption or decryption operation comprising a digital key and a plurality of scrambling bits intermixed with the digital key, through the multiplexer, from the plurality of input/output registers to a key register~~;~~, and ~~transmitting~~ storing the scrambling bits ~~to a~~ in the scrambling register of the plurality of input/output registers; and

B1

processing the message data with a processor receiving the data from the input register, receiving the digital key data from the key register, and the scrambling bits from the scrambling register, and outputting the corresponding message data to an output register.

Claim 31 (canceled).

32. (Currently amended) A method according to Claim 30, wherein the scrambling bits are ~~transmitted~~ intermixed with the digital key randomly.

33. (Currently amended) A method according to Claim 30, wherein the scrambling bits are transmitted to the scrambling register whenever digital key data is input into the plurality of input/output registers.

In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**

B1

34. (Previously added) A method according to Claim 30, wherein the scrambling bits comprise groups of eight bits.